Number Theory: a brief history with a view towards Hilbert's 12th Problem

Cristian D. Popescu, University of California San Diego

The University of Edinburgh, June 2024

What is Number Theory?

C. F. Gauss (1777–1855): "Number Theory is the queen of Mathematics, while Mathematics is the queen of all the Sciences."

We cannot argue with Gauss!

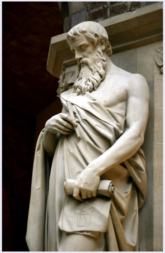
He ranks among history's most influential mathematicians. In 1798, at the age of 21, Gauss wrote **"Disquisitiones Arithmeticae" ("Arithmetical Investigations")**, a brilliant textbook on number theory whose logical structure set the standard for later texts in mathematics. It had a revolutionary impact on number theory, making it truly rigorous and systematic and paving the path for modern number theory.

How old is number theory and what is it about?

Origins

At its origins, number theory began as an effort to understand the properties of positive integers $1, 2, 3, 4, \cdots$. Our ability to count dates back to prehistoric times. Very near the dawn of civilization, people had grasped the idea of "multiplicity" and thereby had taken the first steps toward a study of positive integers. So, without any doubt, number theory is one of the oldest branches of mathematics, thousands of years old.

First attempts of a systematic and rigorous study (cca 300 B.C.)



Euclid of Alexandria (cca 300 B.C.): Wrote (compiled) **"The Elements"**, the most influential mathematical text of all times. Books VII–IX (out of 13) are viewed as the first systematic and more or less rigorous treatment of Number Theory.

The Elements (books VII-IX) - the study of "arithmós" (integers greater than 1)

- Euclid defines prime numbers: $2, 3, 5, 7, \cdots$ as those "arithmós" which are only divisible by 1 and themselves and proves (not rigorously) that every "arithmós" can be uniquely written as a product of primes. The primes begin to play a central role in number theory.

- He proves (by contradiction) that the set $\mathcal{P}$ of prime numbers is infinite.

- He defines perfect numbers (teleios arithmós) as those arithmós which equal the sum of their proper divisors and displays the first four perfect numbers:

$$6 = 1 + 2 + 3, \quad 28 = 1 + 2 + 4 + 7 + 14, \quad 496, \quad 8128.$$

- He proved that if p is prime and $(2^p - 1)$ is also prime, then $2^{p-1}(2^p - 1)$ is perfect.

- Note that the primes $p = 2, 3, 5, 7$ do the trick indeed:

$$6 = 2^1(2^2 - 1), \quad 28 = 2^2(2^3 - 1), \quad 496 = 2^4(2^5 - 1), \quad 8128 = 2^6(2^7 - 1).$$

However, note that $p = 11$ does not do the trick because $(2^{11} - 1) = 23 \cdot 89$ is not prime, as proved only in 1536 A.D. by Hudalricus Regius!

Enter L. Euler (1707–1783)

Two millennia later, Euler proved that any even perfect number has to be of the form $2^{p-1}(2^p - 1)$ with p prime and $(2^p - 1)$ prime. This is the Euclid-Euler Theorem.

By 1772 he had proved that $2^{31} - 1 = 2,147,483,647$ is prime. It remained the largest known prime until 1867.

Definition

A prime of the form $(2^p - 1)$, where p is itself prime, is called a Mersenne prime.

Current open problems!

1. Are there infinitely many Mersenne primes? (Conjecturally, the answer is “yes”.)

Comment. At this time, we have only constructed 51 Mersenne primes. The largest known Mersenne prime (and the largest known prime) is:

$$2^{82,589,933} - 1.$$

It has 24, 862, 048 digits. (GIMPS - Great Internet Mersenne Prime Search)

2. Are there any odd perfect numbers? (Conjecturally, the answer is “no”.)

... speaking of Euler...

Euler is considered to be one of the greatest, most prolific mathematicians in history and the greatest of the 18th century. Gauss wrote: “The study of Euler’s works will remain the best school for [all areas of] mathematics, and nothing else can replace it.” Laplace wrote: "Read Euler, he is the master of us all.”

Euler and Calculus

• He was at the forefront of the development of calculus (limits, continuity, differentiation, integration on the real axis) in the 18th century. He made extensive use of infinite series, e.g.

$$\sum_{n=0}^{\infty} \frac{x^n}{n!} = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots = e^x,$$

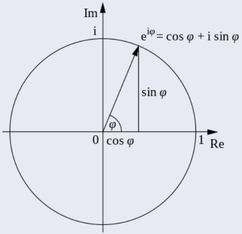
where e is Euler’s number (the base of natural logarithms.)

• He introduced the notation $i := \sqrt{-1}$ (solution to $X^2 + 1 = 0$) and made the first attempts to extend calculus from the real axis $\mathbb{R}$ to the complex plane

$$\mathbb{C} = \{a + ib | a, b \in \mathbb{R}\}.$$

E.g., he extended the infinite series above to all complex numbers x and proved the remarkable equality (now called Euler’s formula)

$$e^{i\varphi} = \cos\varphi + i\sin\varphi, \qquad \text{for all real numbers } \varphi.$$



...speaking of Euler...

Euler's formula: $e^{i\varphi} = \cos\varphi + i\sin\varphi$

Note that if n is a positive integer, then the special value $\zeta_n = e^{i\frac{2\pi}{n}}$ of Euler's exponential function e^x is a root of the equation $X^n - 1 = 0$:

$$\zeta_n^n = e^{i2\pi} = \cos 2\pi + i\sin 2\pi = 1 + i\cdot 0 = 1.$$

It is easy to see that the full set of solutions to $X^n - 1 = 0$ is given by the following special values of e^x:

$$\{\zeta_n^0, \zeta_n^1, \zeta_n^2, \dots, \zeta_n^{n-1}\}.$$

We call ζ_n a primitive n–th root of unity.

... speaking of Euler

Euler introduced analytic (calculus) methods to number theory

- He introduced the most important (and mysterious) function in number theory, the zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \qquad \text{for all } s \in \mathbb{R}_{>1},$$

studied its special values $\zeta(2k)$ at even positive integres $2k$, proving in 1731 the remarkable equality

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = \frac{\pi^2}{6}.$$

- He sensed that ζ "knew" the mysterious prime numbers, by proving the Euler product formula:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathcal{P}} \frac{1}{1 - p^{-s}}.$$

- He proved that the series of inverses of primes diverges (stronger than the infinitude of $\mathcal{P}$!):

$$\sum_{p \in \mathcal{P}} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \cdots = +\infty.$$

- He wondered about questions regarding the distribution of primes, paving the road to the statement and proof of the famous prime number theorem.

Calculus and number theory: Gauss, Riemann

The prime number theorem.

In 1849, Gauss confessed in a letter to a friend that, as a young man (around 1792-1793), he had thought about the number $\pi(x)$ of primes smaller than a given positive real number x. Based on his vast calculations of primes (by hand!) he had conjectured that

$$\pi(x) \sim \int_2^x \frac{1}{\log t} dt \sim \frac{x}{\log x}. \qquad \Longleftrightarrow \qquad \lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1.$$

• Gauss's conjecture is now the celebrated prime number theorem, proved by Jacques Hadamard and Charles Jean de la Vallée Poussin in 1896, by using methods of complex analysis (calculus on the complex plane) and the Euler–Riemann zeta function ...

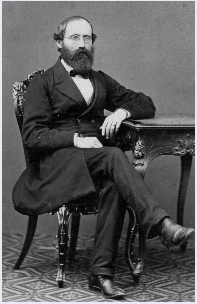
• The prime number theorem states in a very precise way that the primes are sparsely distributed among the integers. The probability of running into a prime between 1 and x is $\frac{1}{\log x}$ which approaches 0 as x approaches ∞. No wonder large primes are so hard to find!

• Open Question: How good is the approximation $\pi(x) \sim \frac{x}{\log x}$? The magnitude of the error term is expected to be that of $\sqrt{x}\log x$, but that is equivalent to the Riemann Hypothesis!

B. Riemann (1826-1866)

• In his dissertation (1851), he laid the geometric foundations for complex analysis (calculus on the complex plane) through a theory of what we now call Riemann surfaces. The analytic foundations of complex function theory had been laid out by A. L. Cauchy in the 1820s.

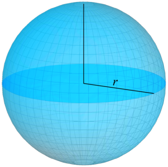
• In 1859, publishes "On the Number of Primes Less Than a Given Magnitude", a 9 page landmark paper in number theory. In it, he achieves many things:

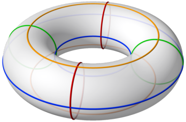


1. Extends Euler's zeta function $\zeta(s)$ to an analytic (complex–differentiable) function at all complex numbers $s \neq 1$. This is what we call now the Riemann zeta function.
2. Proves that $\zeta(s)$ admits an internal symmetry (functional equation):
$$\zeta(s) \sim \zeta(1-s).$$
3. Establishes an intimate relationship between $\zeta(s)$ and Gauss's prime counting function $\pi(x)$. This lies at the foundation of the proof of the prime number theorem.
4. Uses the functional equation to show that the so called trivial solutions of $\zeta(s) = 0$ are $-2, -4, -6, \ldots$.
5. States the Riemann Hypothesis (viewed today as one of the most important unsolved problems in mathematics): the non–trivial solutions of $\zeta(s) = 0$ lie on the vertical line $s = 1/2 + it$ with $t \in \mathbb{R}$.

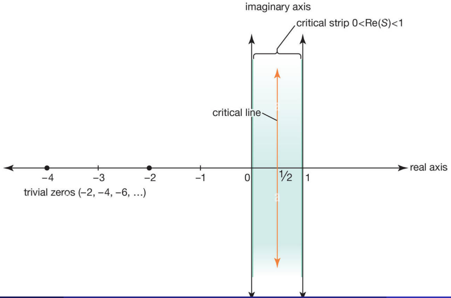
... speaking of Riemann ...

Examples of compact Riemann surfaces (Sphere and Torus)





The Riemann Hypothesis



Calculus + Algebra and Number Theory: Dirichlet

G. L. Dirichlet (1805-1859)

- He started considering deeper, more refined questions about the distribution of primes (based on hints by Euler and Legendre in the previous century!).

- If a and m are two positive, coprime integers, are there infinitely many primes in the following arithmetic progression?

$$a, \quad a + 1 \cdot m, \quad a + 2 \cdot m, \quad a + 3 \cdot m, \quad \dots$$

If so, what is the proportion (density) of such primes among all the primes?

- He introduced algebraic gadgets (functions, now called Dirichlet characters) $\chi : \mathbb{Z} \longrightarrow \mathbb{C}$ which satisfy

$$\chi(a) = \chi(b) \text{ if } m|(a-b), \quad \chi(a \cdot b) = \chi(a) \cdot \chi(b), \quad \chi(a) = 0 \text{ if } \gcd(a, m) \neq 1.$$

- He used χ to construct new (twisted) versions of the Riemann zeta function

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \qquad s \in \mathbb{C} \text{ with } Re(s) > 1,$$

now called Dirichlet L–functions.

...speaking of Dirichlet...

- By studying the analytic properties of these L–functions, he proved the following beautiful theorem.

Theorem (Dirichlet, 1837)

There are infinitely many primes in the arithmetic progression

$$a,\, a+m,\, a+2m\,,\, a+3m,\, \dots .$$

Their density among all the primes is $\frac{1}{\phi(m)}$, where $\phi(m) = |\{a \in \mathbb{Z} | 1 \leq a \leq m, \quad \gcd(a, m) = 1\}|$ is the Euler totient function.

A few comments

- For example, take $m = 4$. Then, Dirichlet's theorem states that exactly $1/2$ of the primes give you remainder 1 when divided by 4 and the other $1/2$ give you remainder 3.

- Dirichlet tells us that there is no bias in the distribution of primes among the $\phi(m)$ distinct arithmetic progressions of ratio m whose first term is coprime to m.

- A vast and extremely far reaching generalization of Dirichlet's theorem on primes in arithmetic progressions was proved by Nikolai Chebotaryov in his thesis in 1922, now known as The Chebotarev Density Theorem. However, for that to happen, many more algebraic methods had to be developed and enter number theory.

Algebra and Number Theory: Kummer and Dedekind

It had become clear since the time of Euler, Gauss, Riemann and Dirichlet that in order to understand the divisibility properties (i.e. the arithmetic properties) of the integers $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$, one had to embed them into larger sets of numbers.

$(\mathbb{Z} \quad \pm \quad \cdot)$ no division! $\mathbb{Z}$ is a ring.	$\subseteq$	$(\mathbb{Q} \quad \pm \quad \cdot \quad \div)$ the rationals $\mathbb{Q}$ form a field	$\subseteq$	$(\mathbb{C} \quad \pm \quad \cdot \quad \div)$ Solve polynomial equations (Gauss, 1799)! $\mathbb{C}$ is an algebraically closed field One can also do calculus (complex analysis) in $\mathbb{C}$

However, from an algebraic (not an analytic) point of view, perhaps going all the way to $\mathbb{C}$ is too much! Most complex numbers (e.g. e, π etc.) are not algebraic over $\mathbb{Q}$, i.e. they are not roots of polynomials with coefficients in $\mathbb{Q}$. So, from an algebraic point of view, considering the subfield $\overline{\mathbb{Q}}$ of $\mathbb{C}$ consisting of all algebraic numbers should suffice.

$$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \overline{\mathbb{Q}} \subseteq \mathbb{C}, \qquad \sqrt{2},\ \sqrt[3]{5},\ e^{\frac{2\pi i}{n}} \in \overline{\mathbb{Q}}, \text{ roots of } X^2 - 2 = 0, \quad X^3 - 5 = 0, \quad X^n - 1 = 0.$$

- However, $\overline{\mathbb{Q}}$ is still too large for algebraic purposes (it is infinite dimensional as a vector space over $\mathbb{Q}$.)

- Fortunately, $\overline{\mathbb{Q}}$ is the union of its subfields K which can be obtained from $\mathbb{Q}$ by adjoining a single root of a polynomial with coefficients in $\mathbb{Q}$. These are the number fields - the main objects of study of algebraic number theory. Here are some examples:

$$K = \mathbb{Q}(i) = \{a + bi | a, b \in \mathbb{Q}\}, \qquad \dim_{\mathbb{Q}} \mathbb{Q}(i) = 2, \qquad K = \mathbb{Q}(\zeta_n), \qquad \dim_{\mathbb{Q}} \mathbb{Q}(\zeta_n) = \phi(n).$$

- Every number field K contains a distinguished subring (no division!) $\mathcal{O}_K$, called its ring of algebraic integers, similar in some respects to $\mathbb{Z}$. Here are some examples:

$$\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}, \qquad \mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\},$$

$$\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n] = \{a_0 + a_1\zeta_n^1 + a_2\zeta_n^2 + \dots \mid a_i \in \mathbb{Z}\}.$$

E. Kummer (1810-1893). Fermat's Last Theorem and Ideal Numbers.

- As part of his efforts to solve Fermat's equation $X^n + Y^n = Z^n$, for $n \geq 3$, Kummer observed that it is better to do calculations in the ring of algebraic integers $\mathbb{Z}[\zeta_n]$ rather than $\mathbb{Z}$ itself. Here is why:

$$X^n = Z^n - Y^n = \prod_{k=0}^{n-1}(Z - \zeta_n^k \cdot Y), \qquad \text{where } \zeta_n = e^{\frac{2\pi i}{n}}.$$

- Unfortunately, although one can define prime elements in $\mathbb{Z}[\zeta_n]$, this ring fails to satisfy the unique factorization property which $\mathbb{Z}$ satisfies. In other words, not every element in $\mathbb{Z}[\zeta_n]$ which is not invertible can be written uniquely as a product of primes.

- If this had been the case, Kummer would have proved Fermat's Last Theorem purely algebraically by 1844! ... We had to wait until 1995 for a full solution by British mathematicians Andrew Wiles and Richard Taylor, a tour de force in modern Number Theory, involving methods from Algebra, Geometry, Complex and p–adic Analysis, Representation Theory etc.

- In 1844, after a letter exchange with Dirichlet, Kummer proved that $\mathbb{Z}[\zeta_{23}]$ does not satisfy unique factorization (is not a UFD, a unique factorization domain, in modern language.) Today, we know that there are exactly 30 rings $\mathbb{Z}[\zeta_n]$ which are UFDs and $n = 23$ is the smallest value for which this fundamental property fails.

...speaking of Kummer

- Kummer was tenacious: by introducing the notion of "ideal number", he developed subtle methods to study what prevents $\mathbb{Z}[\zeta_p]$ from being a UFD, for a prime number p. He defined the notion of a regular prime and proved Fermat's Last Theorem for infinitely many exponents n, those which are divisible by at least a regular prime.

Note. Now, we know that there are infinitely many irregular primes. The smallest is 37 (found by Kummer.) The current conjecture (C. L. Siegel, 1964) is that $e^{-1/2} \sim 60\%$ of all primes are regular.

Kummer's work made that the ring of integers $\mathcal{O}_K$ in a number field K is only very rarely a Unique Factorization Domain. Also, it was clear that the obstruction to unique factorization in this ring must be a very subtle and worth studying invariant of the field K.

R. Dedekind (1831-1916). Ideals and a new kind of Unique Factorization.

- In 1863 (with added supplements to the 1879 and 1894 editions) Dedekind published Dirichlet's lectures on number theory as "Vorlesungen uber Zahlenteorie" ("Lectures on Number Theory"), about which it has been written that

> *"Although the book is assuredly based on Dirichlet's lectures, and although Dedekind himself referred to the book throughout his life as Dirichlet's, the book itself was entirely written by Dedekind, for the most part after Dirichlet's death."* (Edwards, 1983)

- In the 1879 edition, Dedekind refines Kummer's "ideal numbers" and introduces the notion of ideals in the rings of algebraic integers $\mathcal{O}_K$, as subsets $\mathcal{I} \subseteq \mathcal{O}_K$ which contain 0 and are closed under addition, subtraction, multiplication by arbitrary elements in $\mathcal{O}_K$.

Simplest examples: Principal ideals $a\mathcal{O}_K = \{a \cdot x | x \in \mathcal{O}_K\}$.

All ideals of $\mathbb{Z}$ are principal, of the form $n\mathbb{Z}$, with $n \geq 0$, but that is not the case with most rings $\mathcal{O}_K$, e.g. $\mathcal{O}_K = \mathbb{Z}[\zeta_{23}]$. One can add and multiply ideals, the way one adds and multiplies numbers.

- He defines prime ideals in $\mathcal{O}_K$ and shows that any ideal $\mathcal{I} \neq 0$ can be uniquely written as a product of non–zero prime ideals.

Example: The non–zero prime ideals of $\mathbb{Z}$ are of the form $p\mathbb{Z}$, where p is a prime number.

This is a new type of unique factorization, for ideals, not for elements in the ring. In modern number theory, rings which satisfy this type of factorization are called Dedekind Domains. So, any ring of algebraic integers $\mathcal{O}_K$ is a Dedekind Domain, but not necessarily a UFD.

... speaking of Dedekind

• The failure of $\mathcal{O}_K$ to be a UFD is due to the fact that not all its ideals are principal ... to measure this failure, one introduces the ideal class group Cl_K of K, consisting of "ideal classes" (two ideals are in the same class if they differ by principal ideals) and endowed with the usual multiplication of ideals. It is a finite, abelian group and it is one of the most important invariants of the number field K.

Note. Revisitng with Kummer: A prime number p is regular if p does not divide the cardinality (the number of elements) in $\mathrm{Cl}_{\mathbb{Q}(\zeta_p)}$. Examples:

$$|\mathrm{Cl}_{\mathbb{Q}}| = 1, \qquad |\mathrm{Cl}_{\mathbb{Q}(\zeta_{23})}| = 3, \qquad |\mathrm{Cl}_{\mathbb{Q}(\zeta_{37})}| = 37.$$

The Dedekind zeta function (Dedekind, 1879)

In the 1879 edition of "Vorlesungen...", the Dedekind zeta–function of a number field K is defined as

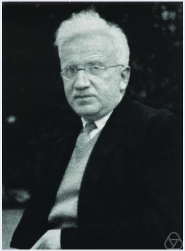
$$\zeta_K(s) = \sum_{\mathcal{I} \subseteq \mathcal{O}_K} \frac{1}{(N\mathcal{I})^s} = \prod_{\mathcal{P} \subseteq \mathcal{O}_K} \left(1 - \frac{1}{(N\mathcal{P})^s}\right)^{-1}, \qquad s \in \mathbb{C} \text{ with } Re(s) > 1,$$

where $\mathcal{I}$ runs through all non-zero ideals of $\mathcal{O}_K$ and $\mathcal{P}$ runs through all non–zero prime ideals of $\mathcal{O}_K$.

Note. This is a vast generalization of the Riemann–Euler zeta function, which is exactly the Dedekind zeta function of the number field $\mathbb{Q}$.

Generalizations of Dedekind's zeta function

E. Hecke (1887-1947): analytic continuation, functional equation, class number formula, Hecke L-functions.



- Following Riemann's ideas, Hecke proved in 1917–1918 that Dedekind's $\zeta_K(s)$ can be analytically continued to $\mathbb{C} \setminus \{1\}$ and it satisfies a functional equation, just like the Riemann–Euler zeta function.

- Building on Dedekind's work, he proved the analytic class number formula on the first non-vanishing derivative of $\zeta_K(s)$ at $s = 0$:

$$\frac{1}{r!} \cdot \zeta_K^{(r)}(0) = -\frac{h_K \cdot R_K}{w_K},$$

where $h_K = |\mathrm{Cl}_K|$ (the class number of K), w_K is the number of roots of unity in K and R_K is the regulator of K (a transcendental quantity). Also, very importantly, r is one less than the number of essential ways in which K can be viewed as a subfield of $\mathbb{C}$ (the number of essentially different complex embeddings of K.)

Example: If $K = \mathbb{Q}$, we have $r = 0$, $R_K = 1$, $h_K = 1$, $w_K = 2$ and the formula reads

$$\zeta_{\mathbb{Q}}(0) = -\frac{1}{2}.$$

- He defined the Hecke L–functions, a vast generalization of Dirichlet's L–functions.

$$L(\psi, s) = \sum_{\mathcal{I} \subseteq \mathcal{O}_K} \frac{\psi(\mathcal{I})}{(N\mathcal{I})^s},$$

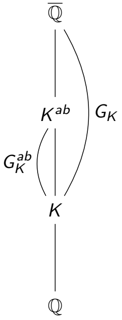
where ψ is a complex valued function (a Hecke character) defined on ideals, generalizing Dirichlet's characters. Hecke proved that these L–functions admit an analytic continuation and satisfy a functional equation, just like Riemann's zeta function.

Galois Theory. Class Field Theory. The Langlands Program.

- Fix a number field K. A field extension $K \subseteq H \subseteq \overline{\mathbb{Q}}$ (denoted H/K in what follows) is called Galois if it is obtained from K by adjoining all the roots of a set of polynomials with coefficients in K.

$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ [all roots $\pm\sqrt{2}$ of $X^2 - 2 = 0$]; $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ [all roots ζ_n^k of $X^n - 1 = 0$]

$\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q}$ [all roots of $X^3 - 2 = 0$], $\overline{\mathbb{Q}}/\mathbb{Q}$ [all roots of all polynomials] .



- The Galois group $G(H/K)$ of a Galois extension H/K is a certain subset of the set of all permutations of the adjoined roots, endowed with the composition of permutations. If this group is abelian (i.e. all these permutations commute with one another), then the extension is called abelian.

$$|G(\mathbb{Q}(\sqrt{2})/\mathbb{Q})| = 2, \text{ abelian}, \qquad |G(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = \phi(n), \text{ abelian ,}$$

$$|G(\mathbb{Q}(\sqrt[3]{2}, \zeta_3)/\mathbb{Q})| = 6, \text{ non-abelian} \qquad |G(\overline{\mathbb{Q}}/\mathbb{Q})| = \infty, \text{ non–abelian.}$$

- For a number field K, the union of all its finite Galois extensions is $\overline{\mathbb{Q}}$. It is a Galois extension of K, whose Galois group $G_K := G(\overline{\mathbb{Q}}/K)$ is infinite and is called the absolute Galois group of K.

- The union K^{ab} of all its finite abelian extensions is called the maximal abelian extension of K. It is a Galois extension of K, whose Galois group $G_K^{ab} = G(K^{ab}/K)$ is an infinite, abelian Galois group.

Class Field Theory - understanding G_K^{ab}.
(1820s-1927, Kronecker, Weber, Hilbert, Takagi, Artin etc.)

Class Field Theory describes the Galois group G_K^{ab} (both algebraically and topologically) in terms of arithmetic properties of K (the arithmetic of ideals $\mathcal{I} \subseteq \mathcal{O}_K$ and all the embeddings of K in $\mathbb{C}$.) In its classical (ideal theoretic) form, this was achieved over a period of 100 years, through the efforts of Kronecker, Weber, Hilbert, Takagi, Artin, among others. More modern approaches followed soon after, with contributions from Hasse, Chevalley, Artin and Tate.

The Langlands Program (1960s, R. Langlands) – understanding G_K?

One of the most important and challenging open problems in number theory and representation theory is understanding the full Galois group G_K. This is the object of the Langlands Program, a conjectural program formulated by R. Langlands in the late 1960s. Although progress has been made over the years, the problem is still wide open.

Hilbert's 12th problem: understanding K^{ab} explicitly

A rather vague question:

Given a number field K, can we find a set of explicit roots of polynomials with coefficients in K which, if adjoined to K, give exactly the maximal abelian extension K^{ab} of K?

L. Kronecker (1823-1891) and H. Weber (1842-1914) - early contributors to class field theory

Theorem (Kronecker–Weber, 1853K, 1886W, 1896H)

The maximal abelian extension $\mathbb{Q}^{ab}$ of $\mathbb{Q}$ can be obtained by adjoining to $\mathbb{Q}$ the special values

$$\zeta_n = e^{\frac{2\pi i}{n}}, \qquad \text{for all } n \in \mathbb{Z}_{\geq 1}$$

of Euler's exponential function $e^z = 1 + \frac{z}{1!} + \frac{z^2}{2!} + \frac{z^3}{3!} + \dots$

Comments:

This is a remarkable theorem for several reasons:

- The values at $\{2\pi i, 2\pi i/2, 2\pi i/3, \dots\}$ of a single analytic function $f(z) = e^z$ generate the infinite extension $\mathbb{Q}^{ab}/\mathbb{Q}$.
- It suffices to solve the equations $X^n - 1 = 0$, for all n, to recover the roots of all abelian polynomial equations over $\mathbb{Q}$.
- Geometric reasons: there is a non–compact (algebraic) torus lurking in the background ...

Kronecker's Liebster Jugendtraum (the dearest dream of his youth), 1880

In a letter to Dedekind, dated March 15, 1880, Kronecker writes about his investigations aimed at fulfilling the "dearest dream of his youth": generating the maximal abelian extensions of all quadratic imaginary fields $\mathbb{Q}(\sqrt{-d})$, for all $d \in \mathbb{Z}_{\geq 1}$, by using special values of what he calls "elliptic functions with singular moduli" instead of Euler's exponential function.

In other words, Kronecker's dream was to prove a Kronecker–Weber type theorem for base fields $\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2}), \dots$. He was aware that the special values of the exponential function would not suffice and he had a replacement in mind.

D. Hilbert (1862-1943) - dreaming big! "We must know, we shall know!"

- On August 8, 1900, in his address to the International Congress of Mathematicians, under the title "Mathematische Probleme", Hilbert formulated a highly influential list of 23 unsolved problems in mathematics. Fourteen of these problems remain unresolved, or partially unresolved to this day.

- Hilbert's 12th Problem can be stated as follows: Prove a Kronecker–Weber type theorem for all base number fields K. In other words, given a number field K, construct complex analytic (meromorphic) functions whose special values generate the maximal abelian extension K^{ab} of K.

Hilbert, Weber's student, was one of the most influential mathematicians of the 19th and early 20th centuries. He discovered and developed a broad range of fundamental areas of mathematics, including invariant theory, the calculus of variations, commutative algebra, algebraic number theory, the foundations of geometry, spectral theory of operators and its application to integral equations, mathematical physics, and the foundations of mathematics. He contributed in an essential way to the development of algebraic number theory and class field theory.

Immediate Progress: Kronecker's dream is fulfilled!

By the end of the 1920s Kronecker's Jugendtraum (Hilbert's 12th Problem for imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$) had been fulfilled, along the lines Kronecker himself had predicted. It gave rise to the theory of "complex multiplication of elliptic modular functions" about which, Hilbert is quoted as having said in 1932 at the ICM Zurich:

> *"The theory of complex multiplication, which forms a powerful link between number theory and analysis, is not only the most beautiful part of mathematics, but of all of science."* **D. Hilbert, 1932**

T. Takagi (1875–1960). $\mathbb{Q}(\sqrt{-1})$

- In his 1901 PhD thesis written under Hilbert's supervision, T. Takagi fulfilled Kronecker's dream for the particular quadratic imaginary field $\mathbb{Q}(\sqrt{-1})$.

- During the following 20 years, Takagi went on to make fundamental contributions to the development of class field theory.

The modular and elliptic functions replace e^z (Takagi, Fueter, Hasse, Deuring etc.)

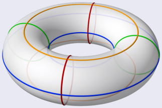
For a given quadratic imaginary fireld $\mathbb{Q}(\sqrt{-d})$ with squarefree d, the correct replacements for e^z are the modular and elliptic functions

$$j(q) = \frac{1}{q} + 744q + 1968884q + 21493760q^2 + \cdots \qquad \wp_d(z) = \frac{1}{z^2} + \sum_{(m,n)\neq(0,0)} \left(\frac{1}{(z-(m\tau_d+n))^2} - \frac{1}{(m\tau_d+n)^2} \right)$$

where $\tau_d = \sqrt{-d}$, if $d \equiv 1, 2 \mod 4$ and $\tau_d = \frac{1+\sqrt{-d}}{2}$, if $d \equiv 3 \mod 4$. The relevant special values are

$$j(e^{2\pi i \tau_d}) \quad \text{and} \quad \wp_d\left(\frac{m+n\tau_d}{k}\right), \text{ for all } m, n, k \in \mathbb{Z}, \text{ such that } m/k \notin \mathbb{Z} \text{ or } n/k \notin \mathbb{Z}.$$

A compact Riemann surface (torus, elliptic curve) is lurking in the background!!!



Recent Progress on Hilbert's 12th Problem: S. Dasgupta and M. Kakde (2023)

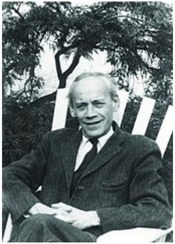
• In 2023, Dasgupta and Kakde announced a solution for Hilbert's 12th Problem for a large new class of number fields: the totally real number fields. Discussing their solution is the main reason why we are gathered in Edinburgh this week.

• Examples of totally real number fields: all the real quadratic fields $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{5})$, ...

• In the process, they had several collaborators, including H. Darmon, R. Pollack, M. Spiess, K. Ventullo, J. Silliman, P. Charollois, J. Wang.

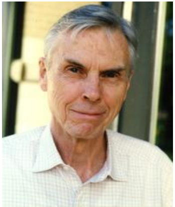
• Dasgupta and Kakde's work builds upon a wide variety of ideas and techniques developed by many people during the past century or so, including: E. Artin, H. Stark, A. Brumer, J. Tate, B. Gross, K. Rubin, H. Darmon, D. Burns, M. Kurihara, T. Sano, J. Ritter, A. Weiss, among others.

... standing on the shoulders of giants ...

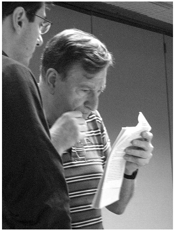


E. Artin

H. Stark



J. Tate



A. Brumer

B. Gross

H. Darmon

A few final comments:

The Dasgupta–Kakde solution to Hilbert's 12th Problem for totally real number fields is very different in spirit from the Kronecker–Weber Theorem or Kronecker's Jugendtraum for several reasons:

1. It makes essential use of a particular type of Hecke L–functions, the abelian Artin L–functions, and certain arithmetic properties of their special values at $s = 0$, as conjectured by Brumer–Stark–Tate–Gross. Harold Stark was the first to suggest in 1976, through both theoretical and numerical evidence, that a link between these special values and Hilbert's 12th problem was plausible.
2. The final explicit construction of the generators of K^{ab} is not complex–analytic in nature (as Hilbert had suggested), but *p*–adic analytic in nature. *P*–adic analysis is a very different type of calculus, non–archimedean in nature, introduced in number theory by K. Hensel in 1897.
3. At least for the moment, there is no geometric object lurking in the background (see the non-compact torus in the Kronecker–Weber case and the compact torus in the Kronecker Jugendtraum case.)

... just scratching the surface...

Are there number fields which are not totally real?

Yes, infinitely many! E.g.: $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{3})$, $\mathbb{Q}(\sqrt[3]{5}), \dots$.

...

"We must know, we shall know!" **(D. Hilbert)**

"The world is full of magical things patiently waiting on our senses to become sharper." **(W.B. Yeats)**